Visual Analytics in Cyber Security

Karolína Burská

Sed molestie commodo augue, a sollicitudin eros egestas vestibulum. Vivamus congue ligula eu massa finibus ullamcorper. Nunc pellentesque mattis enim, sed tempus leo vulputate ac. Proin hendrerit ornare odio. Maecenas mattis sapien placerat ipsum accumsan viverra. Sed imperdiet enim in maximus eleifend. Quisque fringilla quam libero, et porta arcu cursus pretium. Curabitur in nulla eu massa varius pretium eu ultricies lacus. Phasellus viverra urna. Most powerful perception sense? Vision. Sed lacinia sagittis ante et iaculis. Maecenas ac libero tortor. Vivamus dui nibh, facilisis vel mattis eget, viverra non odio. Ut feugiat, diam eget vulputate rutrum, mi lectus pulvinar ipsum, sed luctus velit ligula eu ipsum. Aenean ac leo a leo scelerisque sodales sit amet nec libero. Suspendisse potenti. Morbi tincidunt ex ut egestas vestibulum. Aenean ut leo a nibh faucibus aliquam non id arcu. Proin consequat eu felis quis interdum. Phasellus eu semper tellus. Pellentesque sodales dignissim imperdiet. Integer luctus vehicula purus porttitor tempor. Sed eget commodo orci. Quisque nibh dui, tristique nec quam eget.

Sed molestie commodo augue, a sollicitudin eros egestas vestibulum. Vivamus congue ligula eu massa finibus ullamcorper. Nunc pellentesque mattis enim, sed tempus leo vulputate ac. Proin hendrerit ornare odio. Maecenas mattis sapien placerat ipsum accumsan viverra. Sed imperdiet enim in maximus eleifend. Quisque fringilla quam libero, et porta arcu cursus pretium. Curabitur in nulla eu massa varius pretium eu ultricies lacus. Phasellus viverra urna. Most powerful perception sense? Vision. Sed lacinia sagittis ante et iaculis. Maecenas ac libero tortor. Vivamus dui nibh, facilisis vel mattis eget, viverra non odio. Ut feugiat, diam eget vulputate rutrum, mi lectus pulvinar ipsum, sed luctus velit ligula eu ipsum. Aenean ac leo a leo scelerisque sodales sit amet nec libero. Suspendisse potenti. Morbi tincidunt ex ut egestas vestibulum. Aenean ut leo a nibh faucibus aliquam non id arcu. Proin consequat eu felis quis interdum. Phasellus eu semper tellus. Pellentesque sodales dignissim imperdiet. Integer luctus vehicula purus porttitor tempor. Sed eget commodo orci. Quisque nibh dui, tristique nec quam eget.

Data in Cyber Security

- Structured /semi-structured, unstructured data
- Their transformation into a visual form
- Large amounts of diverse data –> interaction

What is Visual Analytics

- Overview first, zoom/filter, details on demand – *B. Shneiderman*
- Science of analytical reasoning facilitated by visual interactive interfaces
- Based on human cognitive and perceptual principles
- Visual representation of data that enables wider outline from human perspective

Cyber security taxonomies

- All the cyber security data (processes, attacks) or events need to be categorized
- Unification of any existing taxonomies
- Factors as attacker motivation, objectives, tools…

Human & Computer vs. Data

- Differences in **human** and **computer** abilities

Flexibility	x	Storage space
Creativity	x	Processing capacities
Background knowledge	x	Suitable testing environment

Visual Data Exploration Loop

- Combines automatic and visual analysis methods.
- Transforms the data for further exploration.

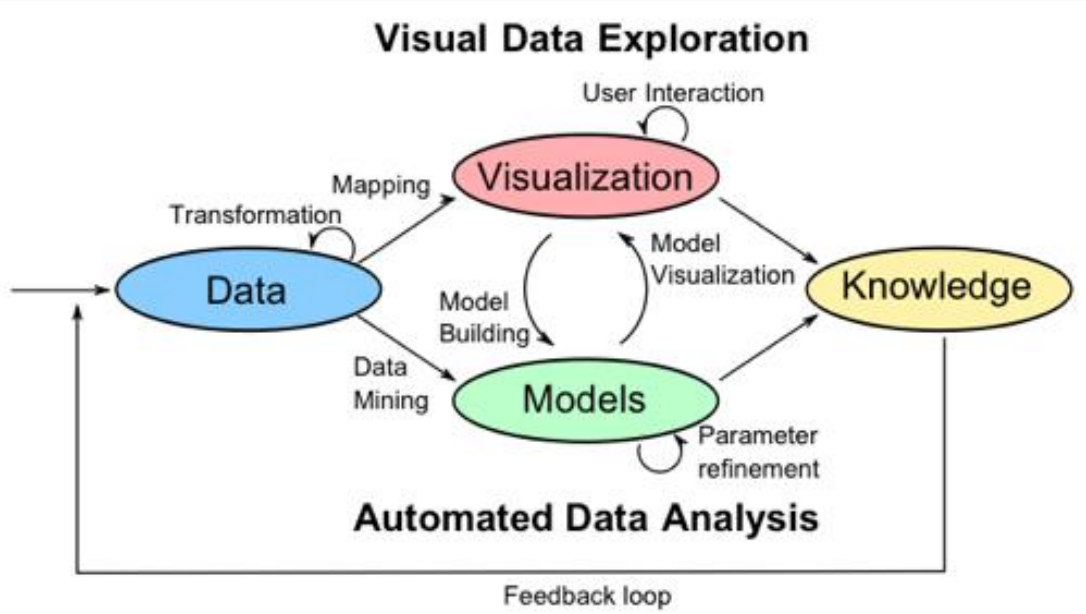

Fig. 1: Visual Data Exploration diagram by D. Keim et al. [2]

Knowledge Generation Model

Human interaction helps to gain knowledge from heterogeneous data sources

Data processing by human vs. computer:

- **computer** – deal efficient and effectively with large amount of data
- **human** – creativity, ability to find subtle connections between data and the problem domain

Both parts are required for the analysis, no clear separation between the two – combination of their strengths.

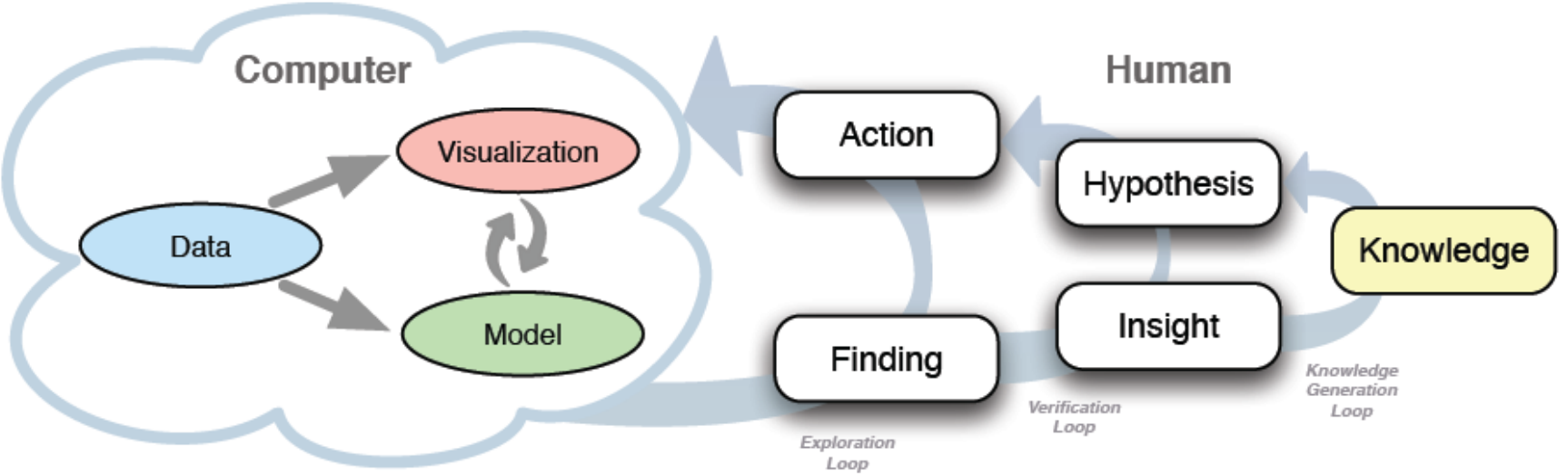

Fig. 1: Knowledge generation model by Sacha et al. [3]

Modified model

Combination of automated analysis techniques with interactive visualizations in context of complex cyber security-related data sets. Derivation of insight from dynamic, ambiguous, and often seemingly conflicting data

- Effective understanding
- Reproducible reasoning

VA can detect the expected and discover the unexpected.

KYPO

Cybernetic Proving Ground (KYPO)

- A project that focuses on simulation of cybernetic threats in an isolated environment
- Provides realistic conditions for various exercises and research
- Enables usage of interactive visualization tools and creation of complex scenarios for specific requirements
- Includes a built-in monitoring infrastructure

Overview – Future Work

- Design of security data (processes, attacks) taxonomies
- Creation of complex formal knowledge base in the form of ontologies
- Adjustments of some existing visualization techniques into a context of cyber security
- Development of interactive tools for visual analysis

References

[1] The kypo - cyber exercise & research platform. **http://www.kypo.cz/,** accessed April 10, 2017.

[2] D. A. Keim, J. Kohlhammer, G. Ellis, and F. Mansmann. *Mastering The Information Age - Solving Problems with Visual Analytics*. Eurographics, 2010.

[3] D. Sacha, A. Stoffel, F. Stoffel, B. C. Kwon, G. Ellis, and D. A. Keim. Knowledge generation model for visual analytics. *IEEE Transactions on Visualization & Computer Graphics*, 20(12):1604–1613, 2014.

[4] J. J. Thomas and K. A. Cook. A visual analytics agenda. *IEEE Computer Graphics and Applications*, 26(1):10–13, Jan 2006.

[5] C. Ware. *Information visualization: perception for design.* Elsevier, 2012.